Cisco Systems

Voice over IP Fundamentals

A systematic approach to understanding the basics of Voice over IP

Jonathan Davidson, CCIE® No. 2560
James Peters

ciscopress.com

Voice over IP Fundamentals

two endpoints. A most-direct-route example is an E-link; if available, this link is the second choice for messages between the (E-link-attached) SSP and the destination SSP.

The SNM function reroutes traffic in the SS7 network. The SMH handles the following during network link failures:

- Linkset rerouting
- Alternate link rerouting
- Traffic flow rerouting to specific endpoints

The SNM process handles the rerouting of traffic through alternate links or linksets during network link failures. The SNM process also controls the flow of traffic to specific endpoints during network link failures.

SNM is divided into three functions:

- Link Management—Monitors and controls the individual links of the signaling endpoint. Link management manages the link interfaces of the signaling endpoint as opposed to the end-to-end link. The link management function is divided into three parts—Link Activation, Link Restoration, and Link Deactivation—described here:
  - The Link Activation process uses the LSSU to inform the adjacent endpoint of the link status. Signaling Link Test Messages (SLTMs) activate links between endpoints. The SLTM acknowledgment (SLTA) restores the link to service and enables traffic to flow over the link.
  - The Link Restoration process uses the LSSU to inform the adjacent endpoint of L3 alignment activities. When the alignment procedures are complete, the link activation process is initiated.
  - The Link Deactivation process places links into alignment procedures when links are failed or in error. Link deactivation uses local MTP2 information and remote information provided by the LSSU to initiate alignment procedures. Link deactivation triggers traffic management procedures when link failures or errors are detected.
- Route Management—Exchanges routing information and status between signaling endpoints. Routing problems are transmitted using transfer messages to redirect traffic during network failure conditions. This enables the other signaling endpoints to choose alternate routes.

  You can use several types of transfer messages for normal and cluster routing management. The functionality and capabilities of these messages are outside the context of this book. The following is a list of the transfer messages used when failures are identified:
  - Transfer Prohibited
  - Transfer Allowed

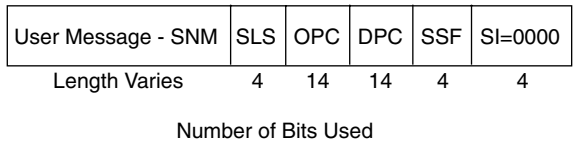
- Transfer Restricted
- Transfer Controlled
- Signaling Route Set and Congestion Test
- Cluster Router Set Test

- Traffic Management—Used to reroute or divert traffic and control congestion during network failure conditions. The traffic management process receives link availability information from SNM Link Management and is advised of routing problems to particular destinations from SNM Route Management. Traffic management also has the capability of advising SMH and the upper-layer protocols of failure conditions. Traffic management uses the following:
  - An interface to SMH to reroute or divert messages over an alternate route
  - Primitives to advise the upper-level protocols about the status of signaling links
  - MSU to transmit messages to SNM peer processes in other signaling points
  - Commands to MTP2 for signaling links

SNM Message Structure

SNM messages transmit and receive network management information between signaling endpoints. SNM uses MTP3 messages (similar to L4 applications) and transmits information in the User Message (UM) field of the MSU. The SNM routing label is illustrated in Figure 4-13.

Figure 4-13 *SNM User—MTP3 Message*



The SI field equals 0000, denoting that the user of this message is network management. The SLS is replaced with the Signaling Link Code (SLC) parameter. The SLC parameter provides the status information of a particular link. If the message does not pertain to any particular link, SLC is set to 0.

Congestion Control

MTP2 monitors the level of messages queued in buffers (both output and retransmission) and alerts SNM in case of congestion.

Onset of congestion messages are sent to SNM when the threshold value for the buffers is exceeded. The SNM process considers all destinations across the link to be congested.

Now consider congestion from the signaling endpoint and STP perspective:

- Signaling endpoints (SSP, SCP) receive congestion information from MTP2 *onset of congestion* indications. Excessive higher-layer messages can cause congestion over signal endpoint (SSP and SCP) links. In this case, SNM sends status messages to applications indicating which DPCs are affected. The application should reduce outgoing messages for a period of time. SNM continues to send the *congestion* status message until MTP2 receives the *end of congestion* indication. At this point, SNM stops sending the status messages, and after the timeout period, user applications resume normal activity.
- If the STP SNM process receives an *onset of congestion* alert concerning a particular link, it considers that the route to its adjacent node is congested. When messages are received for the affected node, the STP SNM process sends a Transfer Controlled (TFC) message to the SNM of the transmitting endpoint. The STP indicates the affected node in the TFC message. This enables the signaling endpoint to choose an alternate route to the affected node. When the SNM process receives the *end of congestion* indication, it stops sending the status indications to the transmitting endpoint.

Rerouting

The SNM rerouting process reroutes traffic around an affected node without causing congestion or losing messages. STPs use this process when the route to a specific endpoint is unavailable. SNM uses the Transfer Prohibited (TFP) message to advise all directly connected nodes of the lost route to the specific endpoint. This enables the other STPs to choose an alternate route to the affected node. When the links are restored, Transfer Allowed (TFA) messages alert the directly connected nodes that normal routing procedures can resume.

Changeover and Changeback

You use changeover procedures when signaling links become unavailable and messages need to be diverted over alternate links. You use changeback procedures when the signaling links become available and normal routing needs to be re-established. Changeover and changeback procedures require SNM actions from both signaling points to maintain sequence and minimize loss.

You initiate the changeover procedure using the *changeover order* (COO) message between the signaling points. The COO message indicates the affected link in the SLC field of the MSU. The SMH function does not select the signaling link identified in the SLC field as the outgoing link. SMH selects an alternate route to reach the adjacent signaling point.

When the receiving point receives the COO message, it selects an alternate route and sends a *changeover acknowledgment* (COA) to the transmitting signaling point. The COO and COA messages contain the FSNs of the last message accepted on the unavailable link. Both signaling points retrieve the messages in the output buffers of the unavailable link and move these messages to the output of the alternate link. At this point, all waiting messages are sent in sequence and without loss, completing the changeover procedure.

You use the changeback procedure when the affected link becomes available. Either signaling point can initiate changeback procedures. SNM advises the SMH process that the messages destined for the alternate link should be stored in the *changeback buffer* (CBB) instead. The *changeback declaration* (CBD) is then sent to the adjacent signaling point identifying that the link is now available. The receiving signaling point responds with a *changeback acknowledgment* (CBA). When the signaling point receives the CBA, SNM advises SMH to send the buffered messages out the primary link and resume normal routing procedures.

SCCP

The SCCP provides network services on top of MTP3: The combination of those two layers is called the Network Service Part (NSP) of SS7. TCAP typically uses SCCP services to access databases in the SS7 network. As illustrated in Figure 4-8, the SCCP provides service interfaces to TCAP and ISUP. SCCP routing services enable the STP to perform Global Title Translation (GTT) by determining the DPC and subsystem number of the destination database.

The following SCCP features are covered in the next few sections:

- Connection-Oriented Services
- Connectionless Services and Messages
- SCCP Management Functions

Connection-Oriented Services

SCCP supports connection-oriented services for TCAP and ISUP, however none of these services is used today. As such, this section does not cover SCCP connection-oriented capabilities, messages, or services.

Connectionless Services and Messages

SCCP provides the transport layer for the connectionless services of TCAP (discussed in the section entitled "Transaction Capabilities Applications Part [TCAP]"). TCAP-based services include 800, 888, 900, calling card, and mobile applications. Together, SCCP and MTP3 transfer non-circuit based messages used in these services. The SCCP also enables the STP to perform GTT on behalf of the end office exchange. The end office exchange views the 800 number as a functional address or, in other words, as a global title address. Because global title addresses are not routed, the SCCP in the end office exchange routes query messages to its home STP.

In this section, connectionless services are based on end office exchanges querying a database to obtain the routing number for an 800 number. The following is an example of how this works in the network.

Together, SCCP and MTP3 transport TCAP 800-based queries to centralized databases. The connectionless messages passed between the SCCP and MTP are called *Unitdata Messages (UDTs)* and *Unitdata Service Messages (UDTSs)* .

The SCCP sends a UDT to transfer subsystem information, and it sends a UDT to perform the GTT function. UDTs also are used to query and receive responses from databases. Table 4-2 lists parameters used in the UDT message.

Table 4-2 *UDT Parameters*

Parameter	Type	Length (Octets)
Message Type	M	1
Protocol Class (PRC)	M	1
Called Party Address (CDA)	M	3 minimum
Calling Party Address (CGA)	M	3 minimum
Subsystem Data	M	Variable

Source: ITU-T Q.713 (7/96)

A UDTS is sent to the originating SCCP advising that the receiving SCCP was unable to deliver the UDT to its destination. The return cause parameter indicates why the UDT is being returned. Table 4-3 lists parameters used in the UDTS.

Table 4-3 *UDTS*

Parameter	Type	Length (Octets)
Message Type	M	1
Return Cause	M	1
CDA	M	3 minimum
CGA	M	3 minimum
Subsystem Data	M	Variable

Source: ITU-T Q.713 (7/96)

SCCP Connectionless Example

This example demonstrates ways you can use SCCP services and messages in a typical 800 call:

1. When the end office switch receives a call setup for an 800 number, it launches a query to a database. TCAP passes the calling and called address parameters to SCCP, which then fills the appropriate fields in the UDT and sets the routing indicator bit indicating that a GTT is required. The SCCP addresses the query to the home STP and passes the message to MTP. MTP in the end office switch creates the MSU and forwards the message to the STP.
2. The SCCP function in the STP receives the query and, using its translation tables, re-addresses the message with the Subsystem Number of the database. The SSN includes the DPC and the database subsystem address. The MTP in the STP then forwards the query to the SCP serving the database.
3. The SCCP in the SCP passes the message to TCAP, which queries the database. The database translates the functional number into the routing number and passes the information to the SCCP, which sets the DPC and sends the response back to the originating end office. The SCCP also sets the routing indicator bit indicating to MTP that the routing should be based on the DPC.

SCCP Management Functions

SCCP management functions maintain the transfer of SCCP messages during failure conditions, including network and subsystem failures. SCCP management processes alert SCCP users, such as TCAP or ISUP, during these failure conditions. SCCP management has interfaces to MTP, SCCP connectionless control, and the subsystems (SCCP users). SCCP management uses the unit data connectionless message format.